Notice of Allowability	Application No.	Applicant(s)	
	09/827,882	BUER ET AL.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed 9/8/06*.

2. ☒ The allowed claim(s) is/are *1-13,15-28 and 31-40*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), ~~Paper No./Mail Date _____~~ P.C.
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 9/8/06 has been entered.

2. Claims 1-13, 15-28, and 31-40 are pending and have been examined.

Drawings

3. The drawings were received on 9-8-06. These drawings are acceptable.

Allowable Subject Matter

4. Claims 1-13, 15-28, and 31-40 are allowed.

5. The following is an examiner's statement of reasons for allowance:

The closest prior art in the field: Silverbrook US 6,334,190, and Bruce Schneier: Applied Cryptography 2nd Edition, Wiley & Sons, Oct. 1985, do not teach the features found in the independent claims of:

In independent claim 1, the use of concurrent multi-round hash operations, implemented in an inner and outer hash engine as disclosed by the applicant, all in combination with the other limitations found in the claim;

In independent claim 9, a hash engine utilized in the multi-round authentication routine of the applicant and having the configuration of a plurality of addition modules comprising a plurality of carry-slave adders each configured to receive a portion of the partial products utilized in the calculation of a final sum;

In independent claims 15 and 31, a hash engine implemented in the SHA1 authentication routine of the applicant comprising five hash-state registers, where the processing comprises four critical and one non-critical data path such that in successive rounds of SHA1 calculations registers implementing a critical path are alternative;

In independent claims 16 and 27, an authentication engine architecture comprising an inner and an outer hash engine able to rearrange multi-round logic so as to reduce the number of hash operations and to schedule addition calculations to be conducted in parallel with multi-round logic operations.

In independent claim 39, a hash engine implemented in authentication engine as disclosed by the applicant comprising the circuit components as found in the claim;

In independent claim 40, a hash engine implemented in an authentication engine as disclosed by the applicant, configured to implement two hash rounds in one computational round, and having the circuit components as found in the claim.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent documents teach systems of cryptographic hashing pertinent to the applicants disclosure:

Sakai et al.	4,754,422
Kindell	4,041,292

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

PEC
9-20-06
Paul Callahan

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER